CVSS FAQ

Q: What is CVSS?

Q: Who developed CVSS?

Q: What does CVSS not do?

Q: What is involved in CVSS?

Q: What are the details of the Base Metrics?

Q: What are the details of the Temporal Metrics?

Q: What are the details of the Environment Metrics?

Q: How is the scoring done?

Q: Is there an easier way to understand all this?

Q: Where can I get the hardcore details of the scoring formulas?

Q: Who is using CVSS?

Q: I am an end-user (CISO/CSO/operations security person), is there anything I need to do?

Q: I am an application or product security vendor, why should I use CVSS and publish CVSS temporal scores?

Q: I am an end-user, and really like other vendors scoring methods, why should I change to CVSS?

Q: What does CVSS really offer that other scoring methodologies do not?

Q: Where can I get the CVSS code?

Q: How can I help establish CVSS through out the industry?

Q: Where can I get more information on CVSS?

Q: What is CVSS?

A: CVSS stands for The Common Vulnerability Scoring System and is a vendor agnostic, industry open standard designed to convey vulnerability severity and help determine urgency and priority of response. It solves the problem of multiple, incompatible scoring systems and is usable and understandable by anyone.

Q: Who developed CVSS?

A: CVSS was commissioned by the National Infrastructure Advisory Council (NIAC) tasked in support of the global Vulnerability Disclosure Framework. It is currently maintained by FIRST (Forum of Incident Response and Security Teams) http://www.first.org/. CVSS was a joint effort involving many groups including:

CERT/CC
Cisco
DHS/MITRE
eBay
Internet Security Systems
Microsoft
Qualys
Symantec

Q: What does CVSS not do?

A: CVSS is not a Threat scoring system (DHS color warning system), a Vulnerability database or a Real-time attack scoring system.

Q: What is involved in CVSS?

A: The CVSS model is designed to provide the end user with an overall composite score representing the severity and risk of a vulnerability. It is derived from metrics and formulas. The metrics are in three distinct categories that can be quantitatively or qualitatively measured. *Base Metrics* contain qualities that are intrinsic to any given vulnerability that do not change over time or in different environments. *Temporal Metrics* contain characteristics of a vulnerability which evolve over the lifetime of vulnerability. *Environmental Metrics* contain those characteristics of a vulnerability which are tied to an implementation in a specific user's environment.

Q: What are the details of the Base Metrics?

A: There are seven Base Metrics which represent the most fundamental, immutable qualities of a vulnerability.

1) Access Vector measures whether a vulnerability is exploitable locally or remotely.

- Local: The vulnerability is only exploitable locally
- Remote: The vulnerability is exploitable remotely (and possibly locally as well)

2) Access Complexity measures the complexity of attack required to exploit the vulnerability once an attacker has access to the target system.

- High: Specialized access conditions exist such as specific window of time (a race condition), specific circumstance (non-default configurations) or victim interaction such as tainted e-mail attachment.
- Low: Specialized access conditions or extenuating circumstances do not exist. In other words, it is always exploitable. This is the most common case.

3) Authentication measures whether or not an attacker needs to be authenticated to the target system in order to exploit the vulnerability.

- Required: Authentication is required to access and exploit the vulnerability.
- Not Required: Authentication is not required to access or exploit the vulnerability.

4) Confidentiality Impact measures the impact on Confidentiality of a successful exploit of the vulnerability on the target system.

- None: No impact on confidentiality.
- Partial: There is considerable informational disclosure.
- Complete: A total compromise of critical system information.

5) Integrity Impact measures the impact on Integrity of a successful exploit of the vulnerability on the target system.

- None: No impact on integrity.
- Partial: Considerable breach in integrity.
- Complete: A total compromise of system integrity.

6) Availability Impact measures the impact on Availability of a successful exploit of the vulnerability on the target system.

- None: No impact on availability
- Partial: Considerable lag in or interruptions in resource availability
- Complete: Total shutdown of the affected resource

7) Impact Bias allows a score to convey greater weighting to one of three impact metrics over the other two

- Normal: Confidentiality Impact, Integrity Impact, and Availability Impact are all assigned the same weight.
- Confidentiality: Confidentiality impact is assigned greater weight than Integrity Impact or Availability Impact.
- Integrity: Integrity Impact is assigned greater weight than Confidentiality Impact or Availability Impact.
- Availability: Availability Impact is assigned greater weight than Confidentiality Impact or Integrity Impact..

Q: What are the details of the Temporal Metrics?

A: There are three Temporal Metrics which represent the time dependent qualities of a vulnerability.

1) Exploitability measures how complex the process is to exploit the vulnerability in the target system.

- Unproven: No exploit code is yet available
- Proof of Concept: Proof of concept exploit code is available
- Functional: Functional exploit code is available
- High: Exploitable by functional mobile autonomous code or no exploit required (manual trigger)

2) Remediation Level measures the level of an available solution.

- Official Fix: Complete vendor solution available
- Temporary Fix: There is an official temporary fix available
- Workaround: There is an unofficial non-vendor solution available
- Unavailable: There is either no solution available or it is impossible to apply

3) Report Confidence measures the degree of confidence in the existence of the vulnerability and the credibility of its report.

- Unconfirmed: A single unconfirmed source or possibly several conflicting reports
- Uncorroborated: Multiple non-official sources; possibly including independent security companies or research organizations
- Confirmed: Vendor has reported/confirmed a problem with its own product

Q: What are the details of the Environment Metrics?

A: There are two Environmental Metrics which represent the implementation and environment specific qualities of a vulnerability.

1) Collateral Damage Potential measures the potential for a loss of physical equipment, property damage or loss of life or limb.

- None: There is no potential for property damage.
- Low: A successful exploit of this vulnerability may result in light property damage or loss.
- Medium: A successful exploit of this vulnerability may result in significant property damage or loss.
- High: A successful exploit of this vulnerability may result in catastrophic property damage and loss.

2) Target Distribution measures the relative size of the field of target systems susceptible to the vulnerability.

- None: No target systems exist, or targets are so highly specialized that they only exist in a laboratory setting (0%)
- Low: Targets exist inside the environment, but on a small scale (1% - 15%)
- Medium: Targets exist inside the environment, but on a medium scale (16% - 49%)
- High: Targets exist inside the environment on a considerable scale (50% - 100%)

Q: How is the scoring done?

A: Scoring is the process of combining all the metric values according to specific formulas.

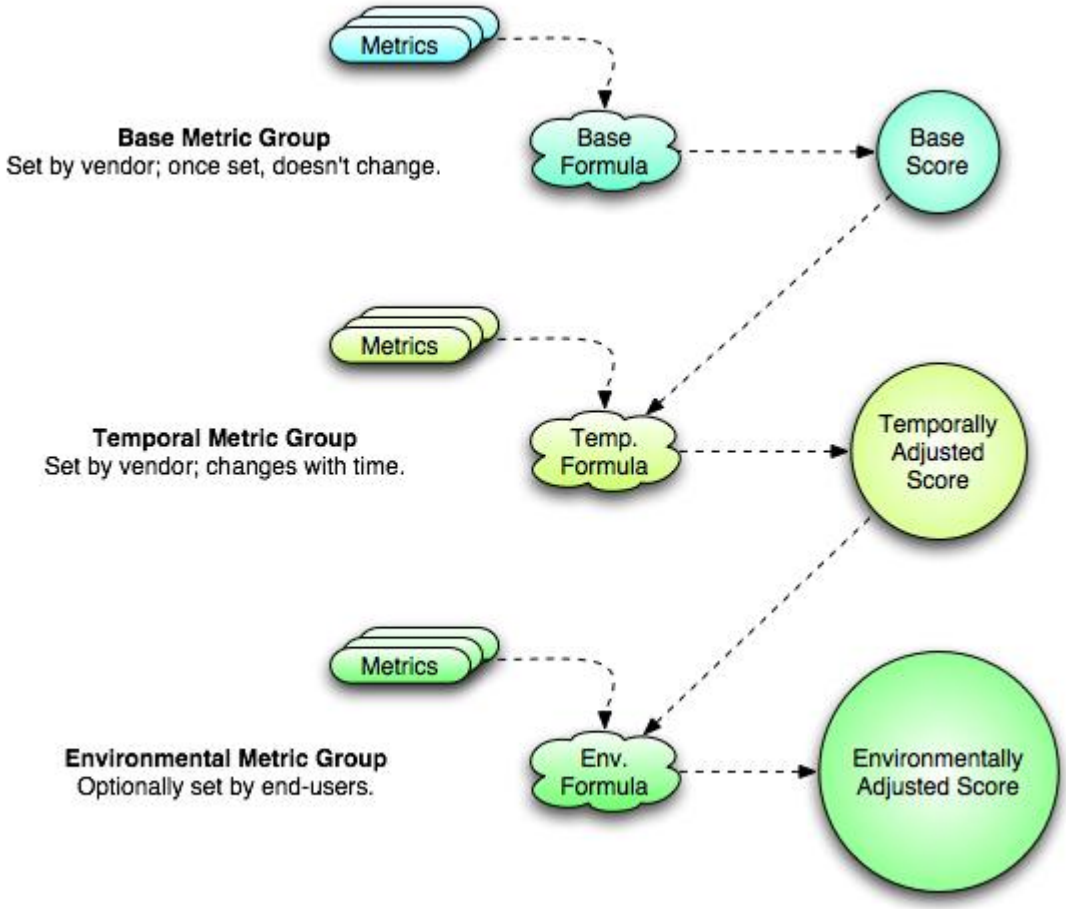
Base Scoring is computed by the vendor or originator with the intention of being published and once set, is not expected to change. It is computed from “the big three” confidentiality, integrity and availability. This is the “foundation” which is modified by the Temporal and Environmental metrics. The base score has the largest bearing on the final score and represents vulnerability ***severity.***

Temporal Scoring is also computed by vendors and coordinators for publication, and modifies the Base score. It allows for the introduction of mitigating factors to reduce the score of a vulnerability and is designed to be re-evaluated at specific intervals as a vulnerability ages. The temporal score represents vulnerability ***urgency*** at specific points in time.

Environmental Scoring is optionally computed by end-user organizations and adjusts combined Base-Temporal score. This should be considered the FINAL score and represents a snapshot in time, tailored to a specific environment. User organizations should use this to ***prioritize responses*** within their own environments

Q: Is there an easier way to understand all this?

A: Yes. This flowchart shows each metric group and how they interrelate with each other.



Q: Where can I get the hardcore details of the scoring formulas?

A: Read the NIAC Paper on CVSS at http://www.first.org/cvss/cvss-dhs-12-02-04.pdf.

Q: Who is using CVSS?

A: NIAC was submitted to the President in January 2005. DHS (Department of Homeland Security) and CVSS developers are encouraging widespread, voluntary adoption. Currently several NIAC member companies (Union Pacific, American Water, Symantec, Akamai) have adopted CVSS with others (CERT/CC, US-CERT, Qualys, Cisco) following.

Q: I am an end-user (CISO/CSO/operations security person), is there anything I need to do?

A: Typically, application and security product vendors will provide both the Base and Temporal scores. As the end user, you need only calculate your Environmental score.

Q: I am an application or product security vendor, why should I use CVSS and publish CVSS temporal scores?

A: As more vendors begin publishing CVSS scores, more customers will understand and appreciate the advantages. They will grow to appreciate the ability to tailor scores to their environment and begin expect CVSS scores of all their suppliers. The more it is used, the better it works.

Q: I am an end-user, and really like other vendors scoring methods, why should I change to CVSS?

A: Other systems are closed competing standards, do not offer a mutable scoring framework, and do not consider different environments.

Q: What does CVSS really offer that other scoring methodologies do not?

A: An open framework that can be used, understood, and improved upon by anybody to score vulnerabilities.

Q: Where can I get the CVSS code?

A: CVSS is a framework that you can use to develop an application suitable to your needs, your environment or your customers. There is no established code as of yet. However here is a sample Excel spreadsheet (zipped), http://www.first.org/cvss/cvss-sample-1.0.zip and also a CVSS web page calculator http://www.patchadvisor.com/PatchAdvisor/CVSSCalculator.aspx.

Q: How can I help establish CVSS through out the industry?

A: Urge your vendors to support CVSS scoring.

Q: Where can I get more information on CVSS?

A: You can get more information at FIRST, the current custodian for CVSS at http://www.first.org/cvss/. Here is also the first NIAC Paper on CVSS at http://www.first.org/cvss/cvss-dhs-12-02-04.pdf.